

17.06.99 EU

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1998年 5月18日

出 願 番 号

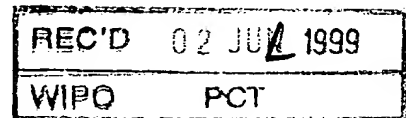
Application Number:

平成10年特許願第135502号

出 願 人

Applicant (s):

三菱マテリアル株式会社



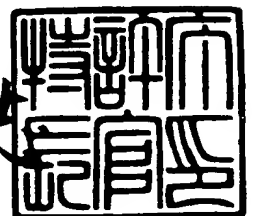
PRIORITY
DOCUMENT

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

1999年 4月 9日

特許庁長官
Commissioner,
Patent Office

伴佐山 建志



出証番号 出証特平11-3021079

【書類名】 特許願

【整理番号】 SOMC0212A

【提出日】 平成10年 5月18日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00
G06F 12/00
H04L 9/00

【発明の名称】 情報共有システム、情報保管装置およびそれらの情報処理方法、並びに記録媒体

【請求項の数】 20

【発明者】

【住所又は居所】 埼玉県大宮市北袋町1丁目297番地 三菱マテリアル株式会社総合研究所内

【氏名】 大久保 達真

【発明者】

【住所又は居所】 埼玉県大宮市北袋町1丁目297番地 三菱マテリアル株式会社総合研究所内

【氏名】 豊田 祥一

【特許出願人】

【識別番号】 000006264

【氏名又は名称】 三菱マテリアル株式会社

【代表者】 秋元 勇巳

【代理人】

【識別番号】 100094053

【弁理士】

【氏名又は名称】 佐藤 隆久

【手数料の表示】

【予納台帳番号】 014890

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9802373

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報共有システム、情報保管装置およびそれらの情報処理方法、並びに記録媒体

【特許請求の範囲】

【請求項 1】 共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能な情報共有システムであって、

少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データを保管可能な情報保管装置と、

情報を見てもよい少なくとも一のメンバーの公開鍵を記憶する記憶部と、情報を暗号化するための共通鍵を用いる上記共通鍵暗号化方式に基づいて入力情報を暗号化して暗号化データを生成する暗号化手段と、暗号化に用いた共通鍵を、上記記憶部に記憶され指定された公開鍵で暗号化し、暗号化鍵を生成する暗号化鍵生成手段と、上記複数の暗号化鍵および暗号化データを上記情報保管装置に転送する転送手段と、上記情報保管装置からグループリストを取得して、当該グループリストのグループ管理者の署名が指定された署名と一致するか否かを判断し、一致する場合にのみ追加するメンバーの公開鍵の登録または脱会するメンバーの公開鍵の削除を行い、追加登録または削除の場合、少なくともグループ管理者の署名、メンバー公開鍵情報を含む新グループリストを作成して上記情報保管装置に転送するリスト管理手段と、上記情報保管装置から所望の暗号化鍵情報および暗号化データを取得して、この暗号化鍵情報から共通鍵を復号し、復号した共通鍵で取得した暗号化データを復号する復号化手段とを有する暗号化復号化装置とを備えた情報共有システム。

【請求項 2】 上記暗号化復号化装置は、上記情報保管装置の共通鍵リストから少なくとも暗号化鍵情報を取得し、この暗号化鍵情報から共通鍵を復号し、復号した共通鍵で上記共通鍵暗号化方式に基づいて入力情報を暗号化して暗号化データを生成し、上記転送手段に出力する手段を

さらに有する請求項 1 記載の情報共有システム。

【請求項 3】 共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくとも

もグループで共通鍵を共有可能で、情報保管装置に少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報共有システムの情報処理方法であって、

グループに属するメンバーを追加登録または削除する場合、上記情報保管装置からグループリストを取得する工程と、

当該グループリストのグループ管理者の署名が指定された署名と一致するか否かを判断する工程と、

一致する場合にのみ、少なくともグループ管理者の署名、メンバー公開鍵情報を含む新グループリストを作成する工程と、

作成したグループリストを上記情報保管装置に転送する工程と

を有する情報共有システムの情報処理方法。

【請求項 4】 共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能で、情報保管装置に少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報共有システムの情報処理方法であって、

グループに属するメンバーで利用する共通鍵を登録する場合、上記情報保管装置からグループリストを取得する工程と、

当該グループリストのグループ管理者の署名が指定された署名と一致するか否かを判断する工程と、

一致する場合にのみ、上記指定されている公開鍵を用いて登録すべき共通鍵を暗号化する工程と、

暗号化された共通鍵を上記情報保管装置に転送する工程と

を有する情報共有システムの情報処理方法。

【請求項 5】 共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能で、情報保管装置に少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管

されている情報共有システムの情報処理方法であって、

上記情報保管装置の共通鍵リストから少なくとも暗号化鍵情報を取得する工程と、

この暗号化鍵情報から共通鍵を復号する工程と、

復号した共通鍵で上記共通鍵暗号化方式に基づいて入力情報を暗号化して暗号化データを生成する工程と、

暗号化されたデータを上記情報保管装置に転送する工程と

を有する情報共有システムの情報処理方法。

【請求項6】 共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能で、情報保管装置に少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報共有システムの情報処理方法であって、

上記情報保管装置から所望の暗号化鍵情報および暗号化データを取得する工程と、

この暗号化鍵情報から共通鍵を復号する工程と、

復号した共通鍵で取得した暗号化データを復号する工程と

を有する情報共有システムの情報処理方法。

【請求項7】 少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報保管装置からグループリストを取得する工程と、

当該グループリストのグループ管理者の署名が指定された署名と一致するか否かを判断する工程と、

一致する場合にのみ、少なくともグループ管理者の署名、メンバー公開鍵情報を含む新グループリストを作成する工程と、

作成したグループリストを上記情報保管装置に転送する工程と

をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 8】 少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報保管装置からグループリストを取得する工程と、

当該グループリストのグループ管理者の署名が指定された署名と一致するか否かを判断する工程と、

一致する場合にのみ、上記指定されている公開鍵を用いて登録すべき共通鍵を暗号化する工程と、

暗号化された共通鍵を上記情報保管装置に転送する工程と

をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 9】 少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報保管装置の共通鍵リストから少なくとも暗号化鍵情報を取得する工程と、

この暗号化鍵情報から共通鍵を復号する工程と、

復号した共通鍵で上記共通鍵暗号化方式に基づいて入力情報を暗号化して暗号化データを生成する工程と、

暗号化されたデータを上記情報保管装置に転送する工程と

をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 10】 少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報保管装置から所望の暗号化鍵情報および暗号化データを取得する工程と、

この暗号化鍵情報から共通鍵を復号する工程と、

復号した共通鍵で取得した暗号化データを復号する工程と

をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 11】 少なくとも複数のメンバーでアクセス可能で、少なくともメンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データを保管可能で、共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能なシステムに適用可能な情報保管装置であって、

グループリスト変更要求に応答して上記グループリストを変更可能なグループリスト管理手段と、

共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録し、共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する共通鍵管理手段と、

暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管し、暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する暗号化データ管理手段とを有する情報保管装置。

【請求項 12】 上記グループリスト管理手段および共通鍵管理手段は、特定グループへのメンバーの新規登録時には、登録時点よりも前にグループで共有されていた情報を読めるように、上記グループリストおよび共通鍵リストを変更する

請求項 11 記載の情報保管装置。

【請求項 13】 上記グループリスト管理手段および共通鍵管理手段は、特定グループへのメンバーの削除時には、削除されたメンバーが当該削除以後グループで共有されていた情報を読めないように、上記グループリストおよび共通鍵リストを変更する

請求項 11 または 12 記載の情報保管装置。

【請求項 14】 少なくとも複数のメンバーでアクセス可能で、少なくともメンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データを保管可能で、共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能なシステムに適用可能な情報保管装置の情報処理方法であって、

グループリスト変更要求に応答して上記グループリストを変更する工程と、
共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録する工程と、

共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する工程と、

暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管する工程と、

暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する工程と

を有する情報保管装置の情報処理方法。

【請求項15】 特定グループへのメンバーの新規登録時には、登録時点よりも前にグループで共有されていた情報を読めるように、上記グループリストおよび共通鍵リストを変更する工程

をさらに有する請求項14記載の情報保管装置の情報処理方法。

【請求項16】 特定グループへのメンバーの削除時には、削除されたメンバーが当該削除以後グループで共有されていた情報を読めないように、上記グループリストおよび共通鍵リストを変更する工程

をさらに有する請求項14または15記載の情報保管装置の情報処理方法。

【請求項17】 グループリスト変更要求に応答して上記グループリストを変更する工程と、

共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録する工程と、

共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する工程と、

暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管する工程と、

暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する工程と

をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能

な記録媒体。

【請求項 18】 グループリスト変更要求に応答して上記グループリストを変更する工程と、

共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録する工程と、

共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する工程と、

暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管する工程と、

暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する工程と、

特定グループへのメンバーの新規登録時には、登録時点よりも前にグループで共有されていた情報を読めるように、上記グループリストおよび共通鍵リストを変更する工程と

をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 19】 グループリスト変更要求に応答して上記グループリストを変更する工程と、

共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録する工程と、

共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する工程と、

暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管する工程と、

暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する工程と、

特定グループへのメンバーの削除時には、削除されたメンバーが当該削除以後グループで共有されていた情報を読めないように、上記グループリストおよび共通鍵リストを変更する工程と

をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 20】 グループリスト変更要求に応答して上記グループリストを変更する工程と、

共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録する工程と、

共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する工程と、

暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管する工程と、

暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する工程と、

特定グループへのメンバーの新規登録時には、登録時点よりも前にグループで共有されていた情報を読めるように、上記グループリストおよび共通鍵リストを変更する工程と

特定グループへのメンバーの削除時には、削除されたメンバーが当該削除以後グループで共有されていた情報を読めないように、上記グループリストおよび共通鍵リストを変更する工程と

をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、複数のユーザ間での情報共有を目的とし、情報の覗き見や改竄を防ぐための情報共有システムおよびその情報処理方法、並びに記録媒体に関するものである。

【0002】

【従来の技術】

近年のコンピュータ・ネットワーク技術の発展に伴い、様々なデジタル情報が

コンピュータネットワーク上で利用されるようになった。

しかし、これらのデジタル情報は、コンピュータ上や、ネットワーク上では、他人の覗き見や改竄が容易である。

そこで、特に秘匿の必要があるユーザのプライベート情報やビジネス情報などは、暗号化技術を利用して暗号化した後、取得、伝達、加工、記録する必要がある。

【0003】

このような秘匿する必要がある情報を暗号化するために、データ暗号規格 (DES ; Data Encryption Standard) などの共通鍵暗号方式が開発された。

この方式では、データを暗号化する暗号鍵をユーザ間で共有するため、他のユーザに暗号鍵が取得されないように、配送、記録する必要があった。

そのため、この暗号鍵を覗き見や改竄、取得されないようにするために、暗号鍵を別の鍵でさらに暗号化した状態の鍵である暗号化鍵として配送する手段が提案されている。

【0004】

ある情報を共有したい複数のユーザがいる場合に、上記の手法で情報を暗号化するには、これらの暗号鍵や暗号鍵を暗号化するための鍵を管理する鍵管理システムや、情報を共有するユーザをグループ化して管理するグループ管理サーバ、情報へのアクセス制御手段などを利用する必要がある。

【0005】

【発明が解決しようとする課題】

このように特定グループで秘匿データを共有する場合の共通鍵管理は、サーバで行われ、このサーバにはサーバ管理者が設けられる。

ところが、このサーバ管理者が当該特定グループに含まれない場合には、何の障害もなくデータを覗くことができることになる。

また、サーバ管理者が当該特定グループに含まれたとしても、一存でグループメンバーを変更することができ、データの管理上、万全であるとはいえない。

【0006】

本発明は、かかる事情に鑑みてなされたものであり、その目的は、暗号化情報

を保管するデータベースや、サーバ、ファイルシステム等の管理者による情報の内容の覗き見や改ざんを防止できる情報共有システムおよびその情報処理方法、並びに記録媒体を提供することにある。

【0007】

【課題を解決するための手段】

上記目的を達成するため、本発明は、共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能な情報共有システムであって、少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データを保管可能な情報保管装置と、情報を見てもよい少なくとも一のメンバーの公開鍵を記憶する記憶部と、情報を暗号化するための共通鍵を用いる上記共通鍵暗号化方式に基づいて入力情報を暗号化して暗号化データを生成する暗号化手段と、暗号化に用いた共通鍵を、上記記憶部に記憶され指定された公開鍵で暗号化し、暗号化鍵を生成する暗号化鍵生成手段と、上記複数の暗号化鍵および暗号化データを上記情報保管装置に転送する転送手段と、上記情報保管装置からグループリストを取得して、当該グループリストのグループ管理者の署名が指定された署名と一致するか否かを判断し、一致する場合にのみ追加するメンバーの公開鍵の登録または脱会するメンバーの公開鍵の削除を行い、追加登録または削除の場合、少なくともグループ管理者の署名、メンバー公開鍵情報を含む新グループリストを作成して上記情報保管装置に転送するリスト管理手段と、上記情報保管装置から所望の暗号化鍵情報および暗号化データを取得して、この暗号化鍵情報から共通鍵を復号し、復号した共通鍵で取得した暗号化データを復号する復号化手段とを有する暗号化復号化装置とを備えている。

【0008】

また、本発明の情報共有システムでは、上記暗号化復号化装置は、上記情報保管装置の共通鍵リストから少なくとも暗号化鍵情報を取得し、この暗号化鍵情報から共通鍵を復号し、復号した共通鍵で上記共通鍵暗号化方式に基づいて入力情報を暗号化して暗号化データを生成し、上記転送手段に出力する手段を、さらに有する。

【0009】

また、本発明は、共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能で、情報保管装置に少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報共有システムの情報処理方法であって、グループに属するメンバーを追加登録または削除する場合、上記情報保管装置からグループリストを取得する工程と、当該グループリストのグループ管理者の署名が指定された署名と一致するか否かを判断する工程と、一致する場合にのみ、少なくともグループ管理者の署名、メンバー公開鍵情報を含む新グループリストを作成する工程と、作成したグループリストを上記情報保管装置に転送する工程とを有する。

【0010】

また、本発明は、共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能で、情報保管装置に少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報共有システムの情報処理方法であって、グループに属するメンバーで利用する共通鍵を登録する場合、上記情報保管装置からグループリストを取得する工程と、当該グループリストのグループ管理者の署名が指定された署名と一致するか否かを判断する工程と、一致する場合にのみ、上記指定されている公開鍵を用いて登録すべき共通鍵を暗号化する工程と、暗号化された共通鍵を上記情報保管装置に転送する工程とを有する。

【0011】

また、本発明は、共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能で、情報保管装置に少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報共有システムの情報処理方法であって、上記情報保管装置の共通鍵リストから少なくとも暗号化鍵情報を取得する工程と、この暗号化鍵情報から

共通鍵を復号する工程と、復号した共通鍵で上記共通鍵暗号化方式に基づいて入力情報を暗号化して暗号化データを生成する工程と、暗号化されたデータを上記情報保管装置に転送する工程とを有する。

【0012】

また、本発明は、共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能で、情報保管装置に少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報共有システムの情報処理方法であって、上記情報保管装置から所望の暗号化鍵情報および暗号化データを取得する工程と、この暗号化鍵情報から共通鍵を復号する工程と、復号した共通鍵で取得した暗号化データを復号する工程とを有する。

【0013】

また、本発明の記録媒体は、少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている上記情報保管装置からグループリストを取得する工程と、当該グループリストのグループ管理者の署名が指定された署名と一致するか否かを判断する工程と、一致する場合にのみ、少なくともグループ管理者の署名、メンバー公開鍵情報を含む新グループリストを作成する工程と、作成したグループリストを上記情報保管装置に転送する工程とをコンピュータに実行させるプログラムが記録されている。

【0014】

また、本発明の記録媒体は、少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報保管装置からグループリストを取得する工程と、当該グループリストのグループ管理者の署名が指定された署名と一致するか否かを判断する工程と、一致する場合にのみ、上記指定されている公開鍵を用いて登録すべき共通鍵を暗号化する工程と、暗号化された共通鍵を上記情報保管装置に転送する工程とをコンピュータに実

行させるプログラムが記録されている。

【0015】

また、本発明の記録媒体は、少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報保管装置の共通鍵リストから少なくとも暗号化鍵情報を取得する工程と、この暗号化鍵情報から共通鍵を復号する工程と、復号した共通鍵で上記共通鍵暗号化方式に基づいて入力情報を暗号化して暗号化データを生成する工程と、暗号化されたデータを上記情報保管装置に転送する工程とをコンピュータに実行させるプログラムが記録されている。

【0016】

また、本発明の記録媒体は、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されている情報保管装置から所望の暗号化鍵情報および暗号化データを取得する工程と、この暗号化鍵情報から共通鍵を復号する工程と、復号した共通鍵で取得した暗号化データを復号する工程とをコンピュータに実行させるプログラムが記録されている。

【0017】

また、本発明は、少なくとも複数のメンバーでアクセス可能で、少なくともメンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データを保管可能で、共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能なシステムに適用可能な情報保管装置であって、グループリスト変更要求に応答して上記グループリストを変更可能なグループリスト管理手段と、共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録し、共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する共通鍵管理手段と、暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管し、暗号化データの取得データに応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送す

る暗号化データ管理手段とを有する。

【0018】

また、本発明では、上記グループリスト管理手段および共通鍵管理手段は、特定グループへのメンバーの新規登録時には、登録時点よりも前にグループで共有されていた情報を読めるように、上記グループリストおよび共通鍵リストを変更する。

【0019】

また、本発明では、上記グループリスト管理手段および共通鍵管理手段は、特定グループへのメンバーの削除時には、削除されたメンバーが当該削除以後グループで共有されていた情報を読めないように、上記グループリストおよび共通鍵リストを変更する。

【0020】

また、本発明は、少なくとも複数のメンバーでアクセス可能で、少なくともメンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データを保管可能で、共通鍵暗号化方式および公開鍵暗号方式を採用し、少なくともグループで共通鍵を共有可能なシステムに適用可能な情報保管装置の情報処理方法であって、グループリスト変更要求に応答して上記グループリストを変更する工程と、共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録する工程と、共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する工程と、暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管する工程と、暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する工程とを有する。

【0021】

また、本発明では、特定グループへのメンバーの新規登録時には、登録時点よりも前にグループで共有されていた情報を読めるように、上記グループリストおよび共通鍵リストを変更する工程をさらに有する。

【0022】

また、本発明では、特定グループへのメンバーの削除時には、削除されたメンバーが当該削除以後グループで共有されていた情報を読めないように、上記グループリストおよび共通鍵リストを変更する工程をさらに有する。

【0023】

また、本発明の記録媒体は、グループリスト変更要求に応答して上記グループリストを変更する工程と、共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録する工程と、共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する工程と、暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管する工程と、暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する工程とをコンピュータに実行させるプログラムが記録されている。

【0024】

また、本発明の記録媒体は、グループリスト変更要求に応答して上記グループリストを変更する工程と、共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録する工程と、共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する工程と、暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管する工程と、暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する工程と、特定グループへのメンバーの新規登録時には、登録時点よりも前にグループで共有されていた情報を読めるように、上記グループリストおよび共通鍵リストを変更する工程とをコンピュータに実行させるプログラムが記録されている。

【0025】

また、本発明の記録媒体は、グループリスト変更要求に応答して上記グループリストを変更する工程と、共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録する工程と、共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先

に転送する工程と、暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管する工程と、暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する工程と、特定グループへのメンバーの削除時には、削除されたメンバーが当該削除以後グループで共有されていた情報を読めないように、上記グループリストおよび共通鍵リストを変更する工程とをコンピュータに実行させるプログラムが記録されている。

【0026】

また、本発明の記録媒体は、グループリスト変更要求に応答して上記グループリストを変更する工程と、共通鍵の登録要求に応答して上記共通鍵リストに要求のあった共通鍵をその暗号化鍵情報を含めて登録する工程と、共通鍵要求に応答して、要求時点、特定グループでの情報共有に最適な共通鍵を選択して、要求先に転送する工程と、暗号化データの登録要求に応答して暗号化データを当該データの暗号化に用いられた共通鍵情報とともに保管する工程と、暗号化データの取得要求に応答して該当する保管暗号化データおよび共通鍵情報を要求先に転送する工程と、特定グループへのメンバーの新規登録時には、登録時点よりも前にグループで共有されていた情報を読めるように、上記グループリストおよび共通鍵リストを変更する工程と、特定グループへのメンバーの削除時には、削除されたメンバーが当該削除以後グループで共有されていた情報を読めないように、上記グループリストおよび共通鍵リストを変更する工程とをコンピュータに実行させるプログラムが記録されている。

【0027】

本発明によれば、複数ユーザが共有したい情報を秘匿しておくために、たとえば共有鍵暗号方式と公開鍵暗号方式が併用される。入力情報は、共有鍵暗号方式で、共通鍵を用いて暗号化される。

【0028】

また、本発明によれば、たとえばネットワーク上での情報共有システムが実現される。

このシステムでは、少なくとも複数のメンバーでアクセス可能な情報保管装置

に、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管される。

【0029】

グループに属するメンバーを追加登録する場合、情報保管装置からグループリストが取得され、取得したグループリストのグループ管理者の署名が指定された署名と一致するか否かを判断される。

そして、一致する場合にのみ、少なくともグループ管理者の署名、メンバー公開鍵情報を含む新グループリストが作成され、作成されたグループリストが情報保管装置に転送され保管される。

【0030】

また、グループに属するメンバーで利用する共通鍵を登録する場合、情報保管装置からグループリストが取得され、取得したグループリストのグループ管理者の署名が指定された署名と一致するか否かを判断される。

そして、一致する場合にのみ、指定されている公開鍵を用いて登録すべき共通鍵が暗号化され、暗号化された共通鍵が情報保管装置に転送され保管される。

【0031】

また、共通鍵を用いてデータを暗号化する場合、情報保管装置の共通鍵リストから少なくとも暗号化鍵情報が取得され、この暗号化鍵情報から共通鍵が復号される。

そして、復号した共通鍵で共通鍵暗号化方式に基づいて入力情報が暗号化されて暗号化データが生成され、暗号化されたデータが情報保管装置に転送され保管される。

【0032】

また、データを復号する場合には、情報保管装置から所望の暗号化鍵情報および暗号化データが取得され、この暗号化鍵情報から共通鍵が復号されり。

そして、復号した共通鍵で取得した暗号化データが復号される。

【0033】

また、情報保管装置では、グループリスト変更要求があると、グループ管理手段により要求に応じたグループリストの変更が行われる。

また、共通鍵の登録要求があると、共通鍵管理手段により、要求のあった共通鍵がその暗号化鍵情報を含めて登録される。また、共通鍵の取得要求があると、共通鍵管理手段により、特定グループでの情報共有に最適な共通鍵が選択されて、要求先に転送される。

また、暗号化データの登録要求があると、暗号化データ管理手段により、暗号化データが当該データの暗号化に用いられた共通鍵情報とともに保管される。また、暗号化データの取得要求があると、暗号化データ管理手段により、保管暗号化データおよび共通鍵情報が要求先に転送される。

【0034】

【発明の実施の形態】

以下、本発明の実施形態を図面に関連付けて詳細に説明する。

【0035】

図1は本発明に係る情報共有システムの基本的な構成図、図2は本発明に係る暗号化復号化装置の構成例を示すブロック図である。

【0036】

本実施形態に係る情報共有システムは、図1に示すように、図2に示す暗号化復号化装置10が組み込まれた第1の端末装置1および第2の端末装置2、並びに暗号化復号化装置10で生成されたグループリストや、共通鍵リスト、暗号化データ等を保管するための情報保管装置としてのWWWサーバ3が、ネットワーク（たとえば、インターネット）4で接続されて構成されている。

【0037】

暗号化復号化装置10は、暗号化部11、共通鍵生成部12、記憶部13、暗号化鍵生成部14、付加情報生成部15、転送部16、署名確認部17、公開鍵管理部18、署名付加部19、並びに復号化部20により構成されている。

そして、署名確認部17、公開鍵管理部18、および署名付加部19を主要素としてリスト管理手段が構成される。

【0038】

暗号化部11は、情報を暗号化するための共通鍵dkまたはWWWサーバ3から読み出した共通鍵ckを用いて、たとえば共有鍵暗号方式（たとえばDES）

により入力情報Mを暗号化して暗号化データM'を生成し、生成した暗号化データM'を転送部16に出力する。

また、暗号化部11は、グループで共通鍵を共有する場合であって、データを暗号化する場合に、特定グループのグループリスト要求、具体的にはグループIDやユーザ公開鍵IDを含むグループリスト要求をWWWサーバ3に対して行う。この要求の転送は転送部16を介して行われる。

【0039】

共通鍵生成部12は、たとえば乱数発生回路等により構成され、情報を暗号化するための共通鍵dkを生成し、暗号化部11および暗号化鍵生成部14に出力する。なお、共通鍵dkは、たとえば64ビットデータとして生成される。

【0040】

記憶部13は、たとえばハードディスクにより構成され、本システムを共有する複数nのユーザ各々の固有の公開鍵PK1, PK2, ..., PKnがあらかじめ記録されており、暗号化鍵生成部14および公開鍵管理部18によりアクセスされる。

【0041】

暗号化鍵生成部14は、暗号化に用いた共通鍵dk（または共通鍵ck）を、記憶部13に記録されているユーザの公開鍵を用い、たとえば公開鍵暗号方式（たとえばRSA）に基づいて暗号化し、1または複数の暗号化鍵EK1, EK2, ..., EKnを生成し、生成した暗号化鍵EK1, EK2, ..., EKnを転送部16に出力する。

また、暗号化鍵生成部14は、特定グループに属するメンバーだけで情報を共有したい場合であって、そのメンバーで利用する共通鍵の登録を行う場合、特定グループのグループリスト要求をWWWサーバ3に対して行う。この要求の転送は転送部16を介して行われる。

【0042】

付加情報生成部15は、たとえば共通鍵dkのメッセージダイジェストkmdをハッシュ関数などで生成し、付加情報ajfとして転送部16に出力する。

なお、付加情報としては、ユーザの秘密鍵で復号化できる暗号化鍵を特定する

ための、ID、ユーザパスワード、証明書、電子メールアドレス、公開鍵、順序情報のうちの、いずれか、もしくは、複数組み合わせた情報であってもよい。

【0043】

転送部16は、入力情報Mの暗号化に伴って生成された1または複数の暗号化鍵EK1, EK2, ..., EK_n、暗号化データM'、および付加情報ajfをネットワーク4を介して情報保管装置としてのWWWサーバ3に転送する。

なお、共通鍵の登録時には転送処理を行わない。

【0044】

署名確認部17は、WWWサーバ3に保管されている特定グループに属する公開鍵のグループリストGLをネットワーク4を介して受けて、グループ管理者のデジタル署名(D署名)を確認し、確認が肯定的である場合、新規にグループに加入するユーザの公開鍵を追加するときは、その公開鍵PKを記憶部13から公開鍵管理部18に出力させ、脱会するメンバーがあるときには受け取ったグループリストに記載されているメンバーから該当メンバーを削除させ、また、共有鍵を登録するときには、公開鍵IDリストに応じた公開鍵PKを記憶部13から暗号化鍵生成部14に出力させる。

【0045】

公開鍵管理部18は、新規にグループに加入するユーザの公開鍵を追加するときに、記憶部13から出力された指定公開鍵PKを受けて、新しいグループリストを作成し、公開鍵番号(N_o)、メンバーの公開鍵をリストに設定し、さらに新規のグループリストに対してグループIDを付加して署名付加部19に出力する。また、たとえば特定グループのグループリスト要求等が発生した場合、この要求をWWWサーバ3に対して行う。

【0046】

署名付加部19は、公開鍵管理部18による新規のグループリストに対してグループ管理者のデジタル署名を付加し、ネットワーク4を介して情報保管装置としてのWWWサーバ3に転送し、登録させる。

【0047】

復号化部20は、特定グループで共通鍵を共有している場合には、WWWサー

バ3に登録されている共通鍵リストCKLの中から所望の共通鍵番号(N o)、暗号化鍵を取得し、公開鍵暗号方式(たとえば、RSA)を用いてユーザの秘密鍵p v kで暗号化鍵を復号して共通鍵を取得し、暗号化部11に出力する。

また、WWWサーバ3に登録されているデータを復号する場合には、データID、公開鍵番号(N o)をWWWサーバ3に転送して、暗号化鍵およびデータを取得し、公開鍵暗号方式を用いて、共通鍵を復号し、共通鍵暗号方式を用いてデータを復号する。

この復号部20は、図3に示すように、暗号化鍵復号化部21、情報復号化部22により構成される。

【0048】

なお、復号化部20は、たとえばWWWサーバ3に複数の暗号化鍵、付加情報、および暗号化データに加えて保管されている共有鍵暗号方式、公開鍵暗号方式のアルゴリズムを識別するためアルゴリズム識別情報desrsa(たとえば、DESとRSAで暗号化した、など)や、暗号化アルゴリズムの実行に必要な上記以外の情報info(たとえば、DESに利用した初期化乱数など)も、取得する。

そして、たとえば、アルゴリズム識別情報desrsa、情報infoに基づいて、復号化に利用できるように、アルゴリズムを初期化する処理等も行う。

【0049】

WWWサーバ3は、図4に示すように、データベースマネジメントシステム(DBMS)31および権限確認機能を有する権限確認部32を有しており、グループリストGL、共通鍵リストCKL、グループの共通鍵リストGCKL、暗号化データリストEDL、およびデータ共通鍵リストDCKLを所定の記憶部に記録し、保管する。

【0050】

DBMS31は、図5に示すように、グループリスト管理部311、共通鍵管理部312、および暗号化データ管理部313の3つの情報管理保管機能を有している。これらの機能は、権限確認機能を利用して、各変更や登録、データ保管要求が権限を満たしているか否かを確認する。

【0051】

グループリスト管理部311は、クライアント側からのグループリスト変更要求時に、グループリストGLにアクセスして、メンバー変更要求に対して応答し、返信されてきたグループ管理者の要求に従ってグループリストGLを変更する。また、グループリスト管理部311は、グループ全体を追加・削除する機能を有している。

【0052】

共通鍵管理部312は、共通鍵登録時に、共通鍵リストCKLとグループの共通鍵リストGCKLにアクセスし、共通鍵の登録を行う。

共通鍵管理部312は、クライアントからの共通鍵要求に対して、その時点・特定グループでの情報共有に最適な共通鍵（特定グループで複数の共通鍵（随時更新されていく）を有している場合には、最新の共通鍵）を選択して、クライアントに転送する。また、たとえば登録対象の共通鍵に関する暗号化鍵、グループID情報を受信したならば、各リストに振り分けて保管する。そのとき、共通鍵IDを生成する。

【0053】

また、特定グループへのメンバーの新規登録時に、新規メンバーが、登録時点よりも前にグループで共有されていた情報を読めるように各リストを変更する場合には、グループリスト管理部311および共通鍵管理部312は協働して以下に示すような処理を行う。

【0054】

この場合、グループリスト管理部311は、権限を確認するとともに、グループIDを参照して特定グループに属するメンバーの公開鍵番号（No）、公開鍵をグループリストGLより取得する。

共通鍵管理部312は、グループの共通鍵リストGCKLよりグループIDを参照して、特定グループで利用されている共通鍵番号（No）を全て検索する。そして、共通鍵リストCKLより、各共通鍵番号（No）とグループ管理者の公開鍵番号（No）が一致する全ての暗号化鍵を取得し、クライアントに転送する。

そして、グループリスト管理部311および共通鍵管理部312は、クライアント側で変更、暗号化等の処理の結果、返信されてきた暗号化鍵とグループリスト、公開鍵番号(N o)と共通鍵IDを受けて、グループリストGL、共通鍵リストCKL、グループの共通鍵リストGCKLを変更する。

これにより、新規追加されたメンバーは、共通鍵リストに自分の公開鍵が含まれているので、過去の共有情報を、取得することができる。

【0055】

また、特定グループからのメンバーの削除時に、削除されたメンバーが、削除以後、グループで共有されていた情報を読めないようにするために各リストを変更する場合、グループリスト管理部311および共通鍵管理部312は、協働して以下に示すような処理を行う。

【0056】

この場合、グループリスト管理部311は、グループリストの更新を行う。最後の返信部分では、新しいグループリストと更新前のグループリストとを比較し、削除したメンバーの公開鍵番号(N o)を割り出し、グループIDと削除したメンバーの公開鍵番号(N o)を共通鍵管理部312にわたす。

共通鍵管理部312は、グループの共通鍵リストGCKLより、グループIDを参照して、特定グループで利用されていた共通鍵番号(N o)を全て検索し、共通鍵リストCKLより、各共通鍵番号(N o)と削除したメンバーの公開鍵番号(N o)が一致する全ての暗号化鍵を削除する。

【0057】

なお、DBMS31では、メンバーの追加と削除が同時に行われた場合には、上述した手法が組み合わされて実行される。

【0058】

暗号化データ保管部313は、共通鍵管理部312と協働して、グループの共通鍵リストGCKL、共通鍵リストCKL、データ共通鍵リストDCKL、暗号化データリストEDLをアクセスし、クライアントの要求に従ってグループリストの送信と暗号化データの受付を行い、データIDを生成する。また、復号化要求を受け取った場合には、データIDと公開鍵番号(N o)を参照し、3つのリ

ストを参照して暗号化データと暗号化鍵を返信する。

【0059】

次に、上記構成による動作を説明する。

なお、ここでは、グループで共通鍵を共有する場合であって、グループへの公開鍵IDの登録例、共通鍵の登録例、データの暗号化および登録例、共通したいユーザを別途指定する場合の暗号化例、並びにデータの復号化例について、図6～図10に関連付けて順を追って説明する。

【0060】

まず、グループで共通鍵を共有する場合であって、グループへの公開鍵IDの登録例について図6に関連付けて説明する。

特定グループに属するメンバーだけで情報を共有したい場合に、まず、グループに属するメンバーの公開鍵IDの登録が行われる。

この場合、アクセス等の権限の確認が行われ、クライアント側（端末側）から特定グループのグループリスト要求がWWWサーバ3に対して、たとえば公開鍵管理部18から行われる（S61）。

【0061】

グループリスト要求に対して、WWWサーバ3から特定グループに属する公開鍵IDリストがネットワーク4を介してクライアント側暗号化復号化装置10に転送される（S62）。

暗号化復号化装置10では、署名確認部17にこの公開鍵リストであるグループリストが入力され、ここでグループ管理者のデジタル署名の確認が行われる（S63）。

確認が肯定的である場合、新規にグループに加入するユーザの公開鍵を追加するときは、その公開鍵PKが記憶部13から公開鍵管理部18に出力され、脱会するメンバーがあるときには受け取ったグループリストに記載されているメンバーから該当メンバーの公開鍵が削除される（S64）。

【0062】

公開鍵管理部18では、記憶部13から出力された指定公開鍵PKを受けて、新しいグループリストが作成され（S65）、公開鍵番号（No）、メンバーの

公開鍵、およびグループIDがリストに設定されて、署名付加部19に出力される。

【0063】

署名付加部19において、公開鍵管理部18による新規のグループリストに対してグループ管理者のデジタル署名が付加される(S66)。

そして、たとえば署名付加部19からグループリスト更新要求がWWWサーバ3に対して行われ、WWWサーバ3においてグループリスト管理部311によりグループリストGLの更新が行われる(S67)。

【0064】

なお、ステップS63において、署名確認が否定的である場合には、当該グループ管理者はグループリスト等の更新、削除等を行う権限のないものとして、ステップS64以降の処理は行われない。

【0065】

次に、グループで共通鍵を共有する場合であって、共通鍵の登録例について図7に関連付けて説明する。

特定グループに属するメンバーだけで情報を共有したい場合に、そのメンバーで利用する共通鍵の登録が行われる。

この場合、アクセス等の権限の確認が行われ、クライアント側(端末側)から特定グループのグループリスト要求がWWWサーバ3に対して、たとえば暗号化鍵生成部14から行われる(S71)。

【0066】

グループリスト要求に対して、WWWサーバ3から特定グループに属する公開鍵IDリストがネットワーク4を介してクライアント側暗号化復号化装置10に転送される(S72)。

暗号化復号化装置10では、署名確認部17にこの公開鍵リストであるグループリストが入力され、ここでグループ管理者のデジタル署名の確認が行われる(S73)。

【0067】

確認が肯定的である場合、公開鍵IDリストに応じた公開鍵PKが記憶部13

から暗号化鍵生成部 14 に出力される。

暗号化鍵生成部 14 では、共通鍵生成部 12 で生成された共通鍵 S k e y 1 が、与えられた公開鍵を用いてたとえば公開鍵暗号方式に基づいて暗号化され、図 7 に示すように、公開鍵番号、メンバー公開鍵を含む共通鍵リスト用データを付加して 1 または複数の暗号化鍵 E K が生成され、転送部 16 に出力される (S 7 4)。

そして、転送部 16 により公開鍵番号、メンバー公開鍵を含む共通鍵リスト用データが付加された暗号化鍵を含む共通鍵リストデータがネットワーク 4 を介して WWW サーバ 3 に転送され、共通鍵管理部 312 により図 7 に示すように所定の場所に保管される (S 7 5)。

なお、転送部 16 から転送される情報には、付加情報生成部 15 で生成された付加情報が含まれる場合もある。

【0068】

なお、ステップ S 7 3 において、署名確認が否定的である場合には、当該グループ管理者は共通鍵の登録を行う権限のないものとして、ステップ S 7 4 以降の処理は行われない。

【0069】

次に、グループで共通鍵を共有する場合であって、データを暗号化する場合について図 8 に関連付けて説明する。

この場合、アクセス等の権限の確認が行われ、クライアント側（端末側）から特定グループのグループリスト要求、具体的にはグループ ID、ユーザ公開鍵 ID（たとえば番号「IC:FF」）の要求が WWW サーバ 3 に対して、たとえば暗号化部 11 から行われる (S 8 1)。

【0070】

グループリスト要求に対して、WWW サーバ 3 から特定グループに属する共通鍵（たとえば「122」）、暗号化鍵（「zxcv」）がネットワーク 4 を介してクライアント側暗号化復号化装置 10 に転送される (S 8 2)。

【0071】

暗号化復号化装置 10 では、復号化部 20 において、共通鍵番号（122）、

暗号化鍵 (z x c v) が取得され、公開鍵暗号方式を用いてユーザの秘密鍵 p v k で暗号化鍵が復号されて共通鍵 S k e y 2 が取得され、暗号化部 1 1 に出力される (S 8 3, S 8 4)。

【0072】

暗号化部 1 1 では、入力情報 M (「こんにちは」) が入力され、この入力情報 M が共有鍵暗号方式 (たとえば、D E S) に基づいて共通鍵 S k e y 2 を用いて暗号化され、共通鍵番号 (1 2 2) が付加された暗号化データ M' (たとえば「jjjjjjjjjjjjjjj」) が生成されて転送部 1 6 に出力される (S 8 5)。

そして、転送部 1 6 により共通鍵番号 (1 2 2) が付加された暗号化データ M' (たとえば「jjjjjjjjjjjjjjj」) がネットワーク 4 を介して WWW サーバ 3 に転送され、暗号化データ管理部 3 1 3 により図 8 に示すように所定の場所に保管される (S 8 6)。

【0073】

次に、共有したいユーザを別途指定する場合であって、データを暗号化する場合について図 9 に関連付けて説明する。

この場合、入力情報 M (「こんにちは」) が暗号化装置 1 0 の暗号化部 1 1 に入力される。このとき、共通鍵生成部 1 2 で、共通鍵 S k e y 1 が生成され (S 9 1)、この共通鍵 S k e y 1 が暗号化部 1 2 および暗号化鍵生成部 1 4 に供給される (S 9 2, S 9 3)。

【0074】

暗号化部 1 1 では、入力情報 M が共有鍵暗号方式 D E S に基づいて共通鍵 S k e y 1 を用いて暗号化され、共通鍵番号 (たとえば「1 2 4」) が付加された暗号化データ M' (たとえば「jjjjjjjjjjjjjjj」) が生成されて転送部 1 6 に出力される。

【0075】

また、暗号化鍵生成部 1 4 によって、ユーザ A、B、C の公開鍵暗号方式 (たとえば、R S A) に基づいた公開鍵 P K が記憶部 1 3 から読み出される。

暗号化鍵生成部 1 4 において、これらそれぞれの公開鍵を利用して、公開鍵暗号方式に基づいて共通鍵 S k e y 1 が暗号化され、たとえば暗号化鍵 (o l k j

、O i w i, X k n m) が得られ、公開鍵番号 (「11:AA」、「1C:FF」、「E5:4B」) を含むデータが転送部16に出力される (S94)。

そして、転送部16により共通鍵番号 (たとえば「124」) が付加された暗号化データM' (たとえば「jjjjjjjjjjjjjjj」)、並びに暗号化鍵 (o l k j, O i w i, X k n m)、公開鍵番号 (「11:AA」、「1C:FF」、「E5:4B」) を含むデータがネットワーク4を介してWWWサーバ3に転送され、図9に示すように所定の場所に保管される (S95)。

【0076】

次に、WWWサーバ3に保管されているデータを取得する場合を、図10に関連付けて説明する。

この場合、たとえば復号化部20からデータID (たとえば「4444」)、公開鍵IDが、WWWサーバ3に対して送信される (S101)。

WWWサーバ3では、受けたデータIDおよびこれに基づく共通鍵番号 (たとえば「122」) により、暗号化データ (たとえば「jjjjjjjjjjjjjjj」) およびこれに対応した暗号化鍵 (z x c v) が暗号化データ管理部313により所定の保管場所から読み出され、ネットワーク4を介してクライアント側へ転送される (S102)。

【0077】

復号化部20では、公開鍵暗号方式を用いて、公開鍵IDに対応した秘密鍵を用いて共通鍵がS k e y 2として復号される (S103)。

そして、この共通鍵S k e y 2を用いて、共通鍵暗号方式に基づきデータが「こんにちは」として復号される (S104)。

【0078】

次に、特定グループへのメンバーの新規登録時に、新規メンバーが、登録時点よりも前にグループで共有されていた情報を読めるように各リストを変更する場合、および特定グループからのメンバーの削除時に、削除されたメンバーが、削除以後、グループで共有されていた情報を読めないようにするために各リストを変更する場合のWWWサーバ3における動作を説明する。

【0079】

まず、特定グループへのメンバーの新規登録時に、新規メンバーが、登録時点よりも前にグループで共有されていた情報を読めるように各リストを変更する場合について説明する。

この場合、WWWサーバ3においては、グループリスト管理部311により、権限が確認されるとともに、グループIDを参照して特定グループ（たとえば、Bチーム）に属するメンバーの公開鍵番号（No）、公開鍵がグループリストGLから取得される。

そして、共通鍵管理部312で、グループの共通鍵リストGCKLよりグループIDが参照され、特定グループ（たとえば、Bチーム）で利用されている共通鍵番号（たとえば、52、111、123）が全て検索される。

さらに、共通鍵管理部312において、共通鍵リストCKLより、各共通鍵番号（たとえば、52、111、123）とグループ管理者の公開鍵番号（たとえば、11:AA）が一致する全ての暗号化鍵（たとえば、qwer、peha、gobp）が取得され、グループ管理者のクライアントに転送される。

【0080】

グループ管理者の暗号化復号化装置10では、グループリストと全ての暗号化鍵を復号化した共通鍵（たとえば、Skey100、Skey105、Skey80）が得られる。図6を参照して説明したように、グループリストの変更が行われた後、それらの共通鍵が、新規登録されたメンバーの公開鍵を利用して暗号化される（たとえば、xhen、mxco、henc）。

そして、これらの暗号化鍵とグループリスト、公開鍵番号（たとえば、L2:CA）と共通鍵ID（たとえば、52、111、123）がWWWサーバ3に送信される。

【0081】

グループリスト管理部311および共通鍵管理部312では、クライアント側で変更、暗号化等の処理の結果、返信されてきた暗号化鍵とグループリスト、公開鍵番号（No）と共通鍵IDを受けて、グループリストGL、共通鍵リストCKL、グループの共通鍵リストGCKLが変更される。

これにより、新規追加されたメンバーは、共通鍵リストに自分の公開鍵が含ま

れているので、過去の共有情報を取得することができるようになる。

【0082】

次に、特定グループからのメンバーの削除時に、削除されたメンバーが、削除以後、グループで共有されていた情報を読めないようにするために各リストを変更する場合について説明する。

【0083】

この場合、WWWサーバ3のグループリスト管理部311では、グループリストの更新が行われる。このとき、最後の返信部分では、新しいグループリストと更新前のグループリストとが比較され、削除したメンバーの公開鍵番号(N o)が割り出される。そして、グループIDと削除したメンバーの公開鍵番号(N o)が共通鍵管理部312にわたされる。

共通鍵管理部312では、グループの共通鍵リストGCKLより、グループIDを参照して、特定グループ(たとえば、Bチーム)で利用されていた共通鍵番号(たとえば、38、444、133)が全て検索される。

次いで、共通鍵管理部312では、共通鍵リストCKLより、各共通鍵番号(たとえば、38、444、133)と削除したメンバーの公開鍵番号(たとえば、LL:BB)が一致する全ての暗号化鍵が削除される。

【0084】

なお、WWWサーバ3、具体的には、DBMS31では、メンバーの追加と削除が同時に行われた場合には、上述した手法が組み合わされて実行される。

【0085】

以上説明したように、本実施形態によれば、少なくとも複数のメンバーでアクセス可能で、少なくともグループ管理者の署名、メンバー公開鍵情報を含むグループリスト、暗号化鍵情報を含む共通鍵リスト、および暗号化データが保管されるWWWサーバ3と、情報を見てもよい少なくとも一のメンバーの公開鍵を記憶する記憶部13と、情報を暗号化するための共通鍵を用いて上記共通鍵暗号化方式に基づいて入力情報を暗号化して暗号化データを生成する暗号化部11と、暗号化に用いた共通鍵を、記憶部に記憶され指定された公開鍵で暗号化し、暗号化鍵を生成する暗号化鍵生成部14と、複数の暗号化鍵および暗号化データをWW

Wサーバ3に転送し保管させる転送部16と、WWWサーバ3からグループリストを取得して、当該グループリストのグループ管理者の署名が指定された署名と一致するか否かを判断し、一致する場合にのみメンバーの公開鍵の追加または脱会するメンバーの公開鍵の削除を上記記憶部に対して行い、追加登録または削除の場合、少なくともグループ管理者の署名、メンバー公開鍵情報を含む新グループリストを作成して上記情報保管装置に転送し保管させるリスト管理手段17, 18, 19と、WWWサーバ3から所望の暗号化鍵情報および暗号化データを取得して、この暗号化鍵情報から共通鍵を復号し、復号した共通鍵で取得した暗号化データを復号する復号化部20とを有する暗号化復号化装置10とをインターネット4で接続したので、グループで共有鍵を共有することができ、暗号化データを保管するデータベースや、サーバ、ファイルシステムの管理者に情報の内容を見られてしまう可能性もない。

したがって、権限のない、サーバ等の情報保管装置の管理者の覗き見、改竄を防ぐことができる。

【0086】

また、本実施形態では、情報保管装置としてのWWWサーバ3に、クライアント側からのグループリスト変更要求時に、グループリストGLにアクセスして、メンバー変更要求に対して応答し、返信されてきたグループ管理者の要求に従ってグループリストGLを変更可能なグループリスト管理部311と、クライアントからの共通鍵要求に対して、その時点・特定グループでの情報共有に最適な共通鍵を選択して、クライアントに転送する共通鍵管理部312と、グループの共通鍵リストGCKL、共通鍵リストCKL、データ共通鍵リストDCKL、暗号化データリストEDLをアクセスし、クライアントの要求に従ってグループリストの送信と暗号化データの受付を行い、データIDを生成し、復号化要求を受け取った場合には、データIDと公開鍵番号(No)を参照し、3つのリストを参照して暗号化データと暗号化鍵を返信する暗号化データ保管部313とを設けたので、暗号化データを保管するデータベースや、サーバ、ファイルシステム等の情報保管装置を利用して共有されるユーザのデータが覗き見されたり、改竄されるおそれもなく、データの管理を確実に行うことができる。

【0087】

なお、暗号化複合化装置 10 におけるグループリストの作成、登録、削除、共通鍵の作成、登録、登録された共通鍵を用いたデータの暗号化、サーバ 3 に登録されたデータの復号処理工程を実行するためのプログラム、あるいはサーバ 3 におけるリストの変更、登録、保管等のプログラムは、第 1 および第 2 の端末装置（コンピュータ）1，2 で読み出し可能な記録媒体、たとえば暗号化装置 10 やサーバ等に設けられたフロッピーディスク、ハードディスク、光ディスク、半導体記憶装置等に記録され、端末装置で読み出されて実行される。

また、他の例としては、たとえばインターネットの専用線や電話回線等の通信線路のように、通信プログラムに伝送する際にこの通信プログラムを一定時間保持するデータ伝送路等を挙げることができる。

【0088】

【発明の効果】

以上説明したように、本発明によれば、グループで共有鍵を共有することができ、暗号化データを保管するデータベースや、サーバ、ファイルシステムのグループ管理者に情報の内容を見られてしまう可能性もない。

【図面の簡単な説明】

【図 1】

本発明に係る情報共有システムの基本的な構成図である。

【図 2】

本発明に係る暗号化復号化装置の構成例を示すブロック図である。

【図 3】

図 2 の復号化部の構成例を示す図である。

【図 4】

WWWサーバの保管される各種リストを示す図である。

【図 5】

本発明に係る情報管理装置としてのWWWサーバにおけるDBMSの詳細な機能を説明するための図である。

【図 6】

グループで共通鍵を共有する場合であって、グループへの公開鍵IDの登録動作例を説明するための図である。

【図7】

グループで共通鍵を共有する場合であって、共通鍵の登録動作例を説明するための図である。

【図8】

グループで共通鍵を共有する場合であって、データを暗号化する場合の動作例を説明するための図である。

【図9】

共有したいユーザを別途してする場合であって、データを暗号化する場合動作例を説明するための図である。

【図10】

復号化動作例を説明するための図である。

【符号の説明】

- 1…第1の端末装置
- 2…第2の端末装置
- 3…WWWサーバ（情報保管装置）
- 4…ネットワーク
- 10…暗号化復号化装置
 - 11…暗号化部
 - 12…共通鍵生成部
 - 13…記憶部
 - 14…暗号化鍵生成部
 - 15…付加情報生成部
 - 16…転送部
 - 17…署名確認部
 - 18…公開鍵管理部
 - 19…署名付加部
 - 20…復号化部

3 1 …データベースマネジメントシステム (DBMS)

3 1 1 …グループリスト管理部

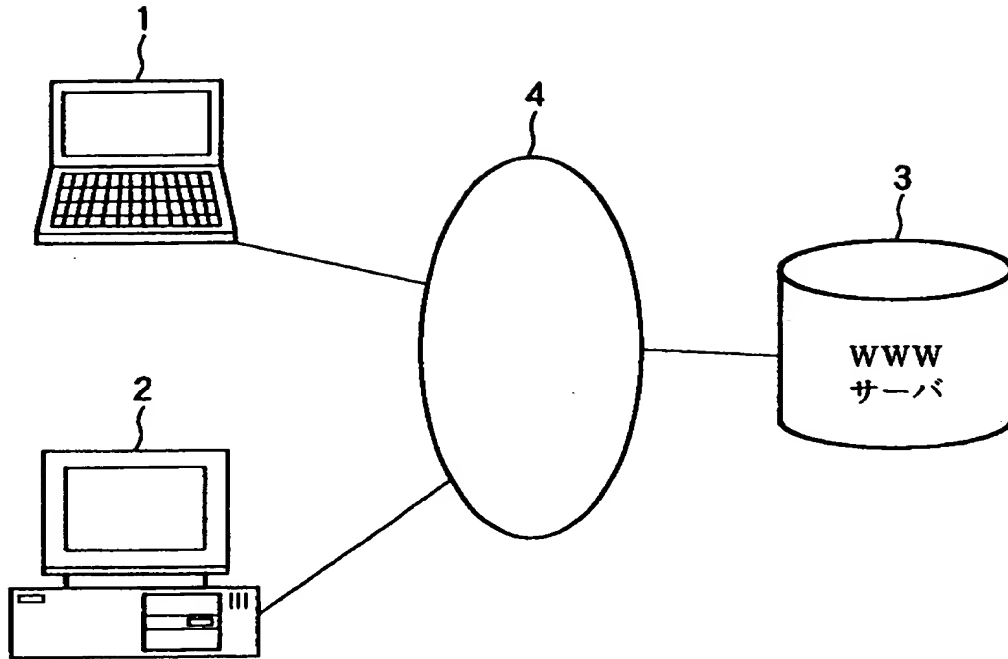
3 1 2 …共通鍵管理部

3 1 3 …暗号化データ管理部

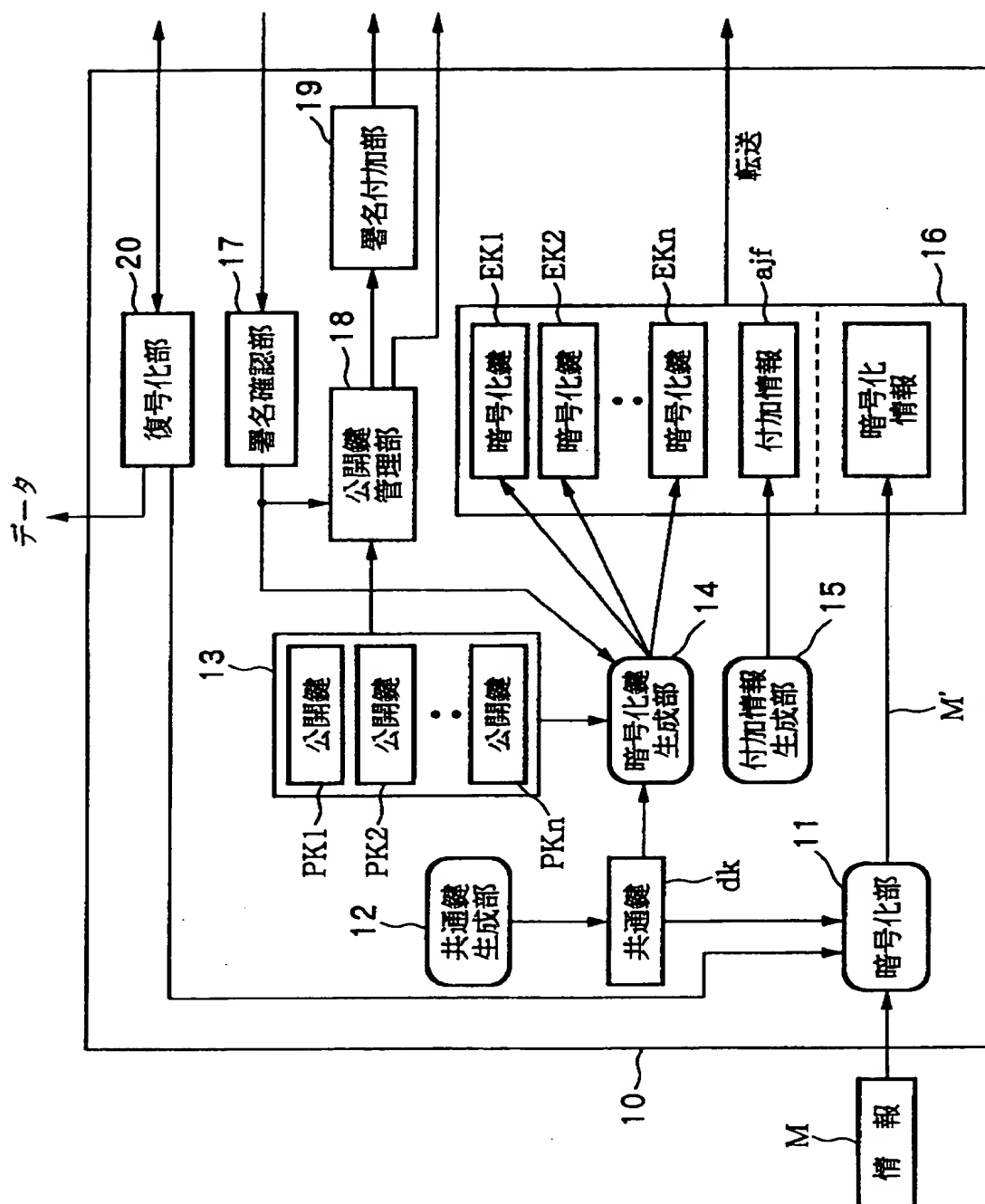
3 2 …権限確認部

【書類名】 図面

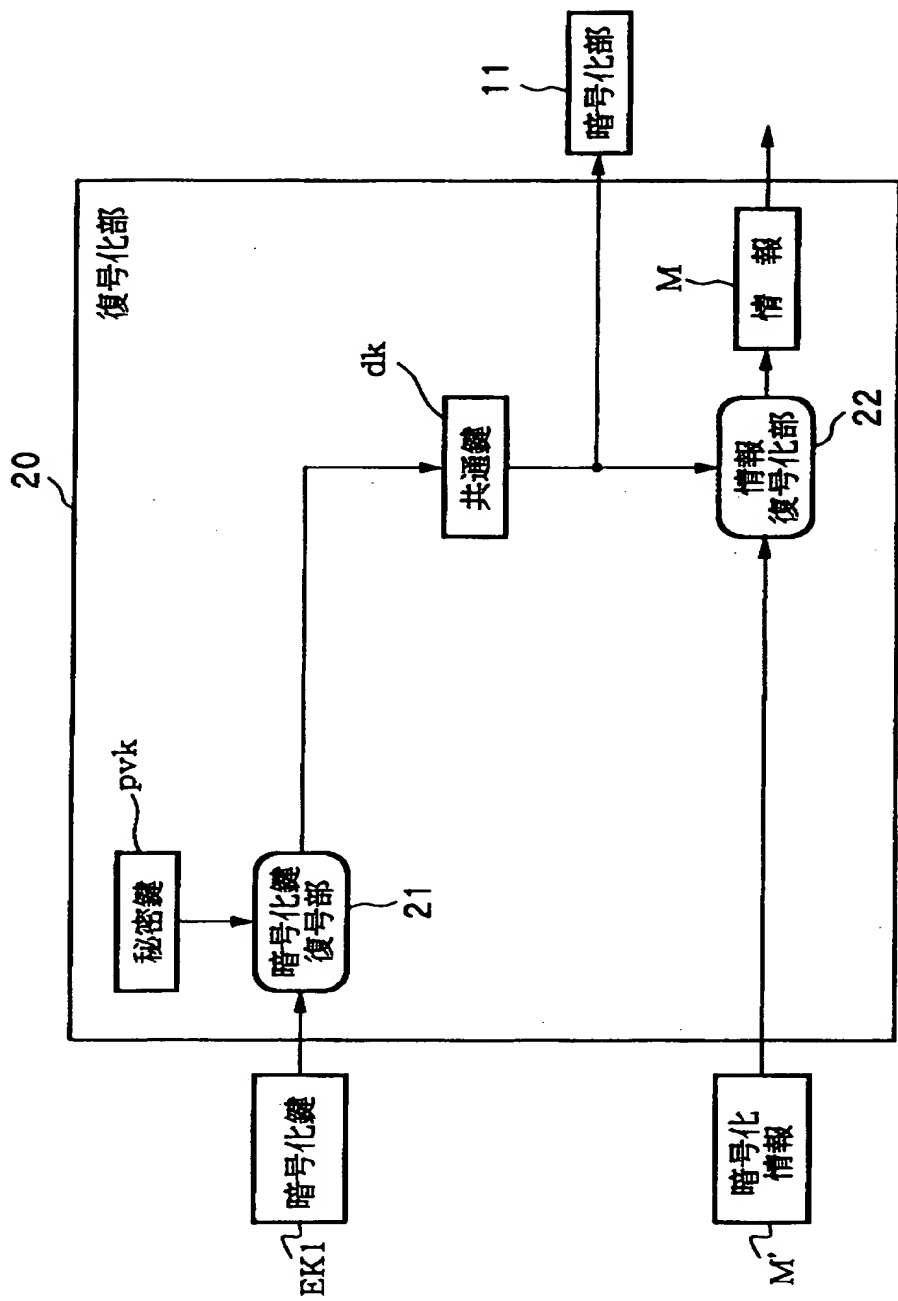
【図 1】



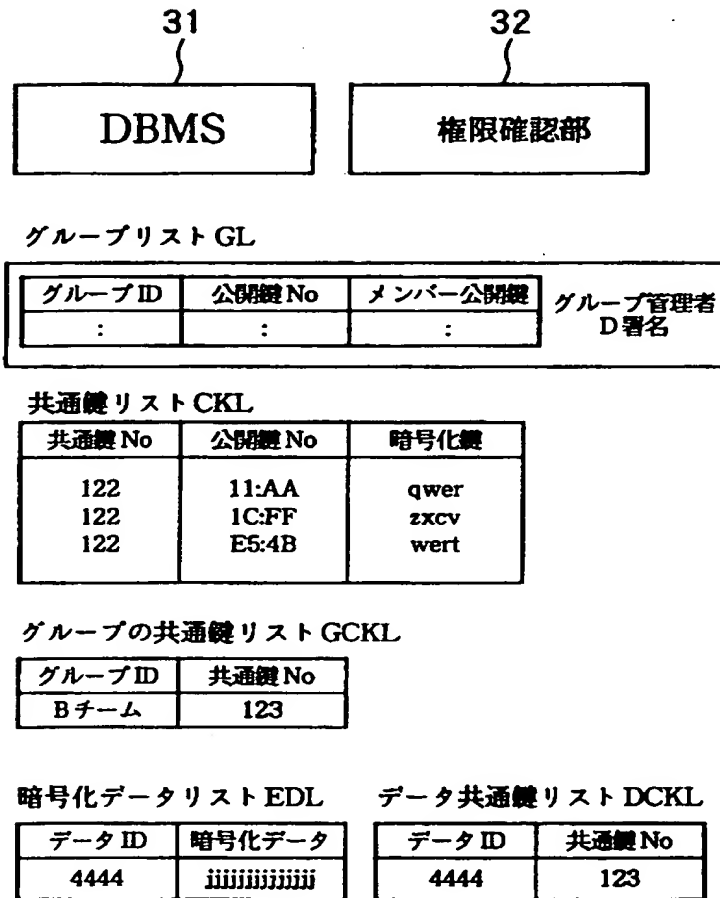
【図 2】



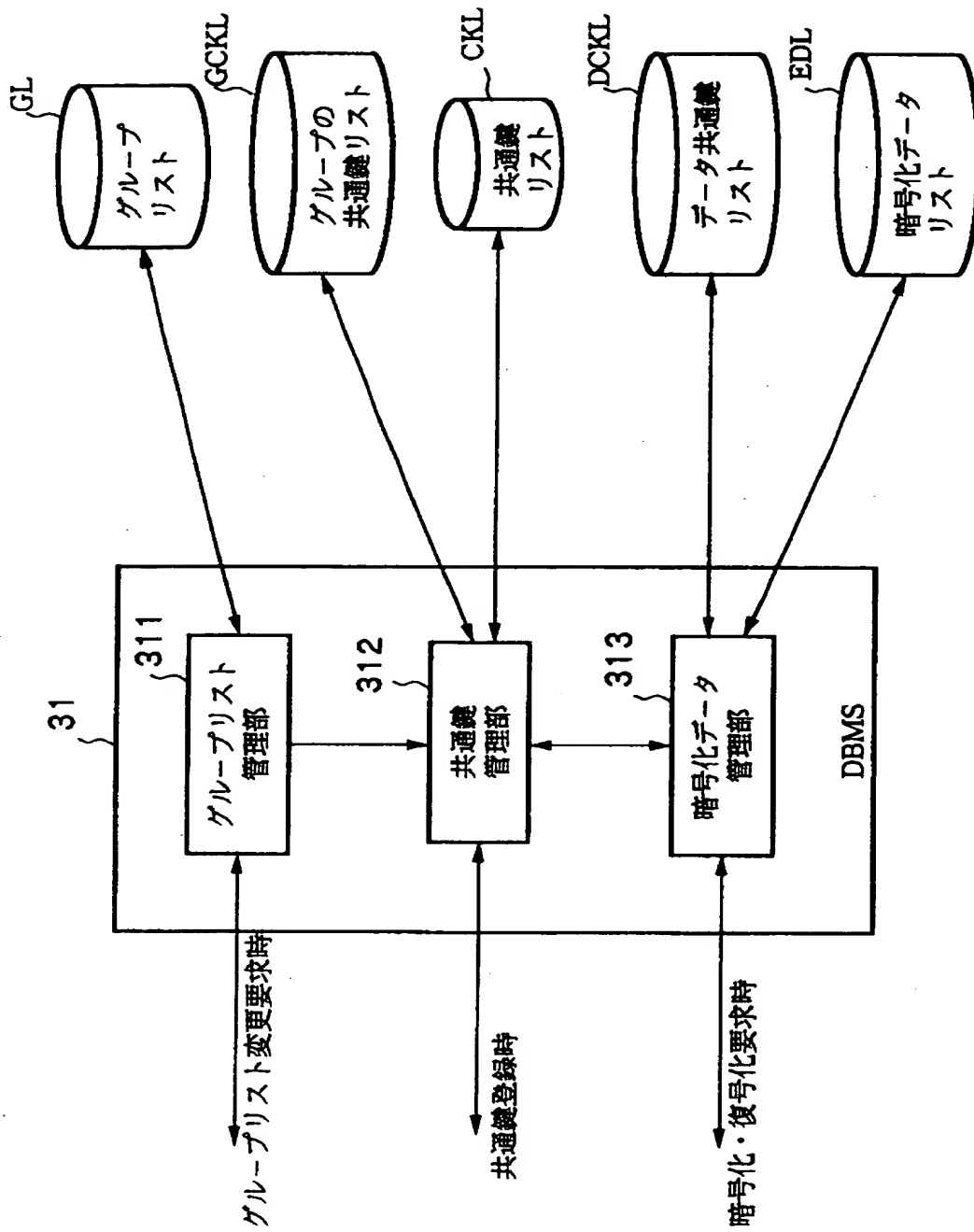
【図 3】



【図 4】

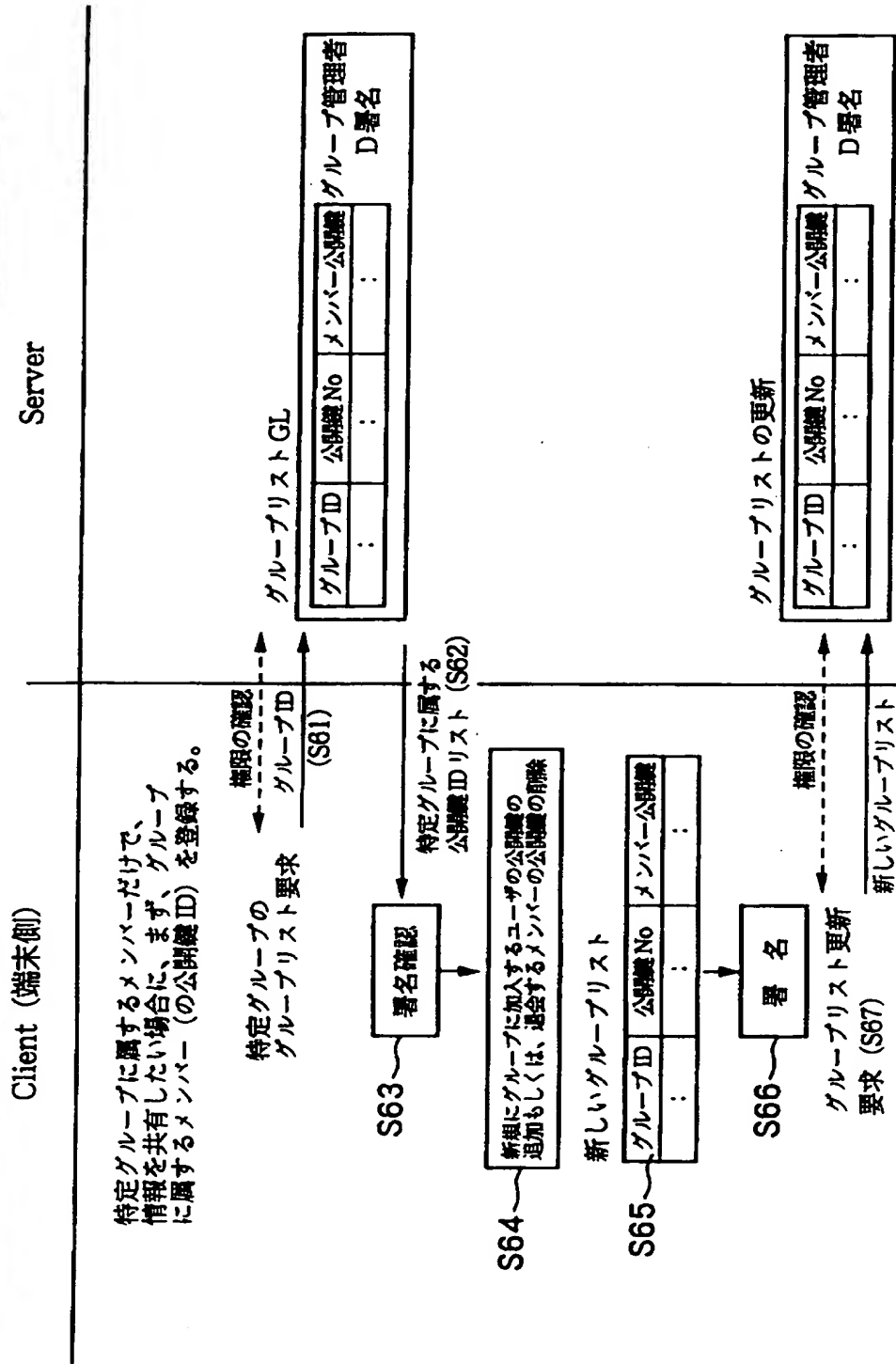


【図 5】

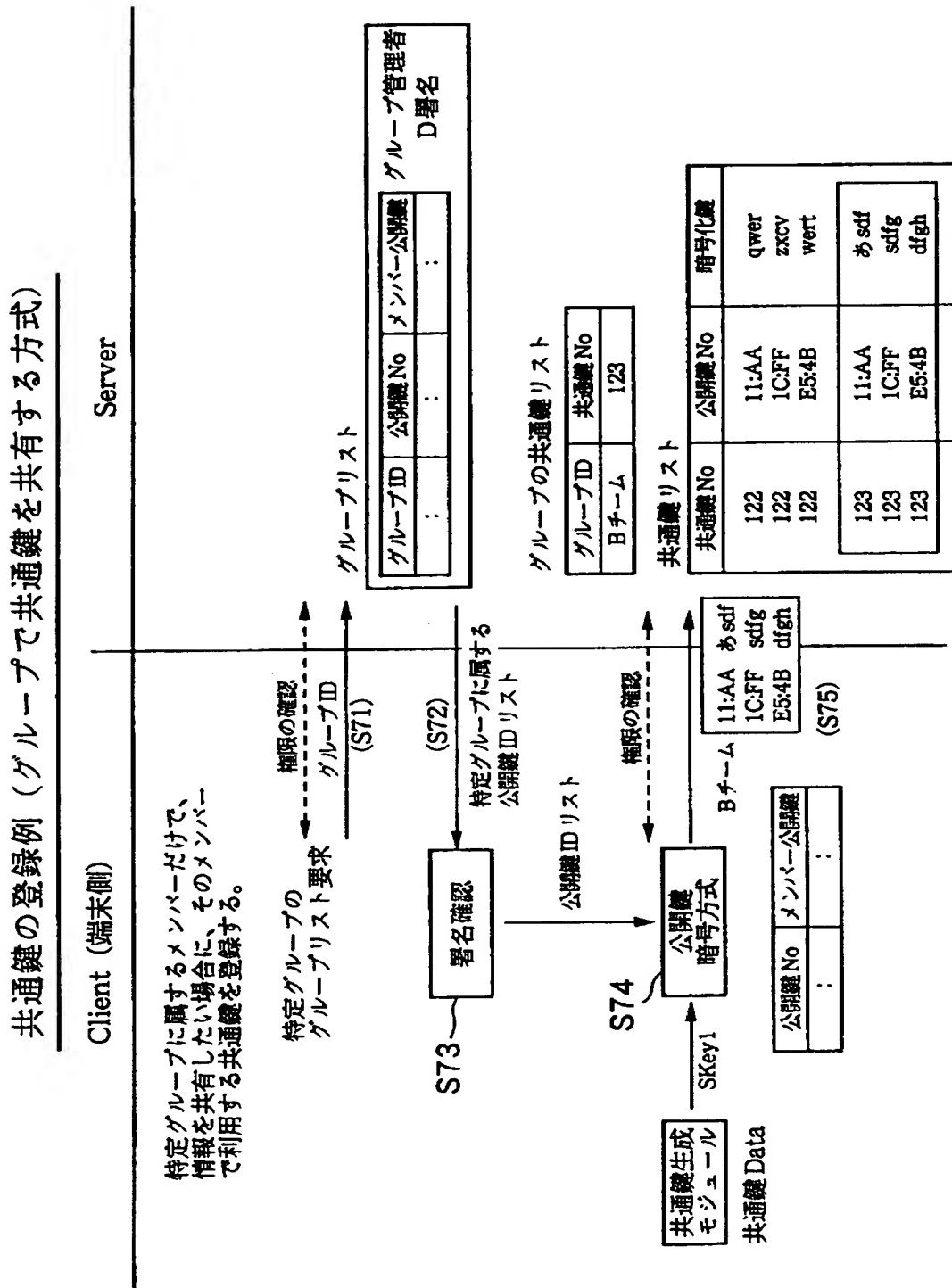


【図 6】

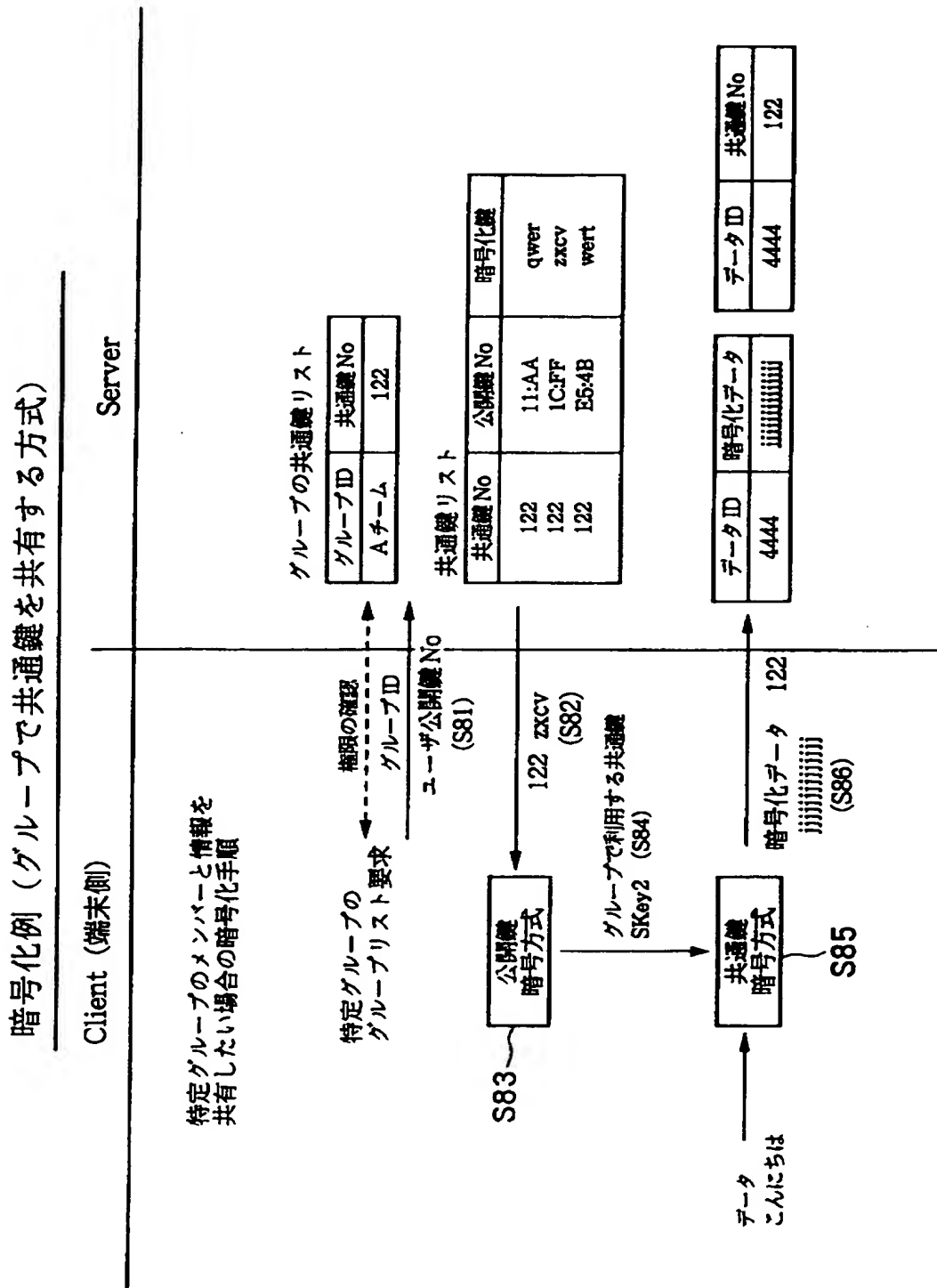
グループへの公開鍵ID登録例（グループで共通鍵を共有する方式）



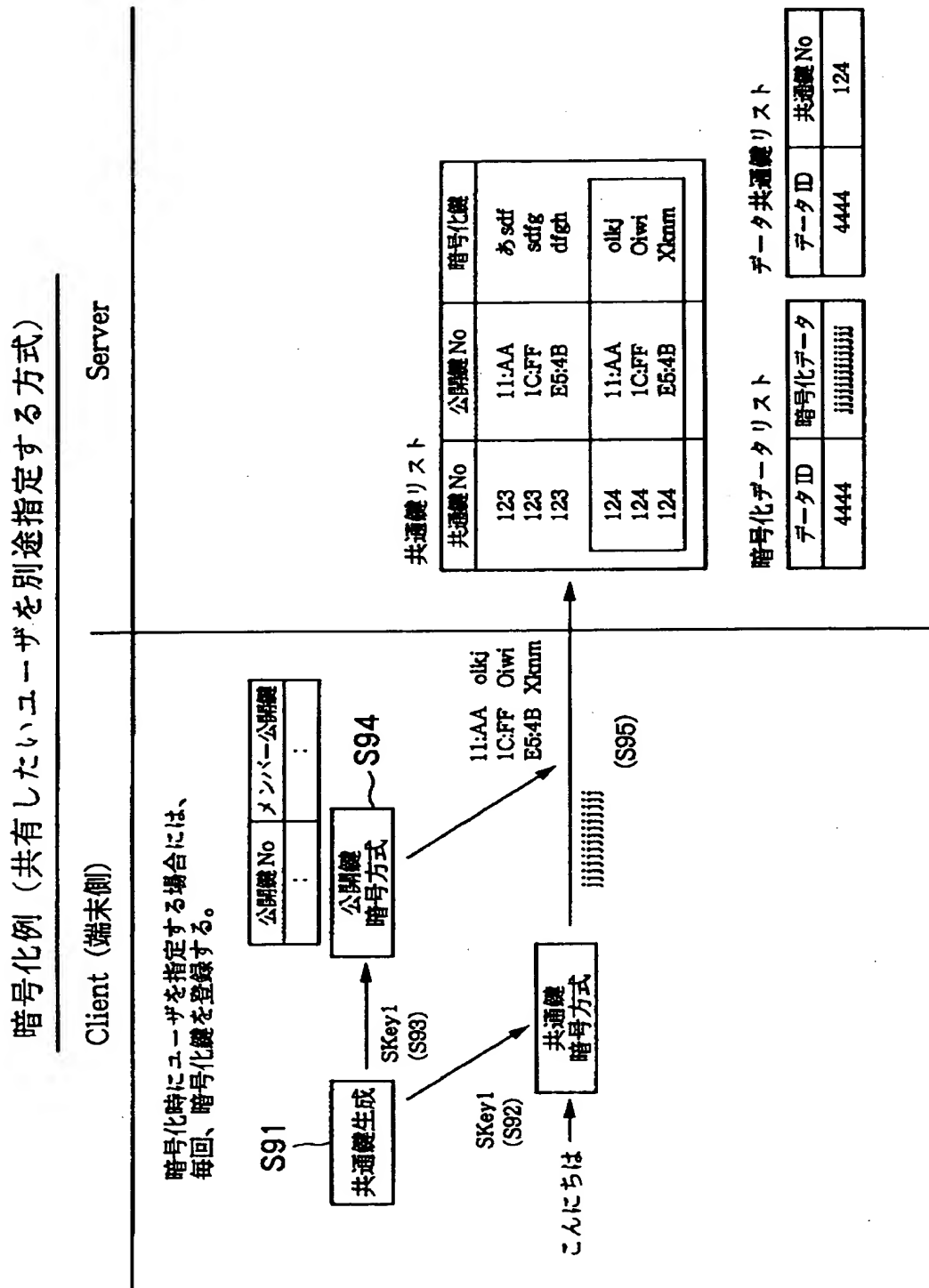
【図 7】



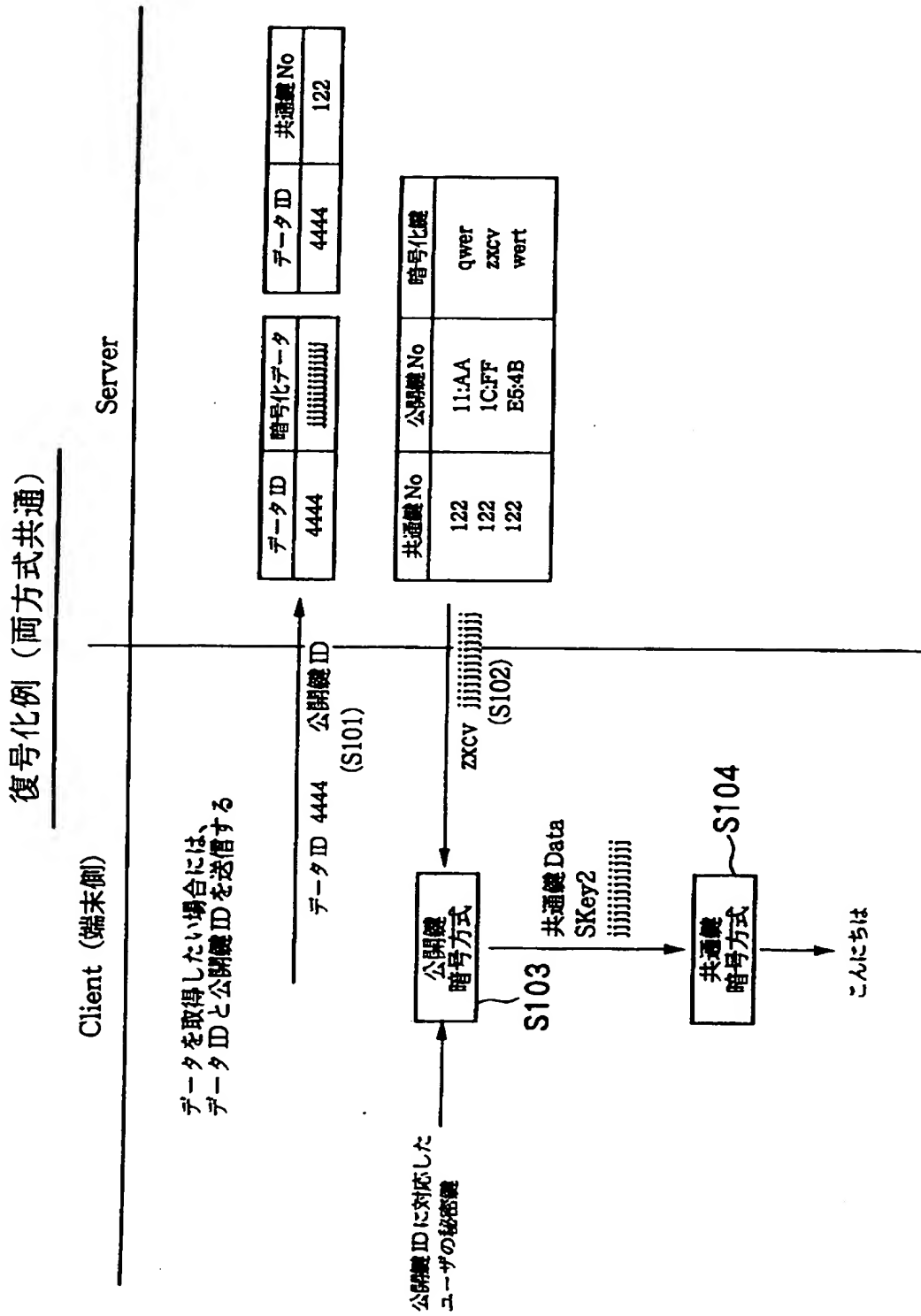
【図8】



【図 9】



【図 10】



【書類名】 要約書

【要約】

【課題】暗号化情報を保管するデータベースや、サーバ、ファイルシステム等の管理者による情報の内容の覗き見や改竄を防止できる情報共有システムおよびその情報処理方法、並びに記録媒体を提供する。

【解決手段】WWWサーバ3からグループリストを取得して、当該グループリストのグループ管理者の署名が指定された署名と一致するか否かを判断し、一致する場合にのみメンバーの公開鍵の追加または脱会するメンバーの公開鍵の削除を記憶部13に対して行い、追加登録または削除を行う場合、少なくともグループ管理者の署名、メンバー公開鍵情報を含む新グループリストを作成してWWWサーバ3に転送するリスト管理手段17、18、19を設ける。

【選択図】 図2

【書類名】

職権訂正データ

【訂正書類】

特許願

<認定情報・付加情報>

【特許出願人】

【識別番号】

000006264

【住所又は居所】

東京都千代田区大手町1丁目5番1号

【氏名又は名称】

三菱マテリアル株式会社

【代理人】

申請人

【識別番号】

100094053

【住所又は居所】

東京都台東区柳橋2丁目4番2号 創進国際特許事務所

【氏名又は名称】

佐藤 隆久

出 願 人 履 歴 情 報

識別番号 [000006264]

1. 変更年月日 1992年 4月10日

[変更理由] 住所変更

住 所 東京都千代田区大手町1丁目5番1号
氏 名 三菱マテリアル株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

This Page Blank (uspto)